Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment on January 15, 2014
2. Standard Drafting Team appointed on January 29, 2014

Description of Current Draft

This draft standard is being posted for an initial comment and ballot. The draft includes modifications to meet the directives of FERC Order No. 791.

Anticipated Actions	Anticipated Date
First 45-Day Comment Period Opens	June 2014
Additional 45-Day Comment Period (if necessary)	August 2014
Final Ballot is Conducted	October/November 2014
Board of Trustees (Board) Adoption	November 2014
Filing to Applicable Regulatory Authorities	December 2014

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	June 2014	Responding to FERC Order No. 791.	Revised

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-6

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-6:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3.3 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

Reliability Standard CIP-003-6 shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date that the standard is approved by an applicable governmental authority, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Where approval by an applicable governmental authority is not required, the standard shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Registered Entities shall not be required to comply with Reliability Standard CIP-003-6, Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of Reliability Standard CIP-003-6.

6. Background:

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

Rationale for Requirement R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale for Requirement R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to low impact BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements by CIP Senior Manager approval of the policies specified in Part 2.1.

The language in Requirement R2, Part 2.4 "external routable protocol paths" and "Dial-up Connectivity" was included to acknowledge the support given in FERC Order No. 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.4 uses the phrase "external routable protocol paths" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. The Standard Drafting Team (SDT) intent in using the phrase "external routable protocol paths" is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).

The additions to Requirement R2, in particular the processes required under Parts 2.2-2.6, address FERC Order No. 791 paragraphs 106-110, which require the standard to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets. The SDT pulled language and concepts from CIP-004, CIP-005, CIP-006, and CIP-008 in order to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2.

In FERC Order No. 791 paragraphs 111-112, FERC upheld that creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome, so the inventory statements remain unchanged.

R2. Each Responsible Entity for its assets containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

CIP-003-6 Table R2 – Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These

delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (R1)	the previous approval. (R1)		months of the previous approval. (R1)
R2	**Operations Planning**	**Lower**	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address one of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 15	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address two of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 16	The Responsible Entity had one or more documented cyber security policies for assets with a low impact rating but failed to address three of the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity did not have any documented cyber security policies for assets with a low impact rating that address the topics as required by Requirement R2, Part 2.1. (2.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 16 calendar months but did complete this approval in less than	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for	calendar months of the previous review. (2.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by Requirement R2, Part 2.1 by the CIP Senior Manager according to Requirement R2, Part 2.1 within 18 calendar months of the previous approval. (2.1) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not reinforce cyber security practices at least quarterly but did reinforce cyber security practices at least every two quarters. (2.6)	or equal to 17 calendar months of the previous approval. (2.1) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include two of the topics as	assets with a low impact rating but failed to include one of the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity documented and implemented one or more processes for assets with a low impact rating but failed to include two of the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity documented and implemented one or more Cyber Security Incident response plans for assets with a low impact rating but failed to include three of the	document or implement any processes for assets with a low impact rating to include the operational or procedural control(s) to restrict physical access as required by Requirement R2, Part 2.2. (2.2) OR The Responsible Entity did not document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.3. (2.3) OR The Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.5 for assets with a low impact rating in less than or equal to 16 calendar months. (2.6)	required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include one of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security	topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity implemented a security awareness program for assets with a low impact rating that reinforced cyber security practices at least quarterly but failed to include two of the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not reinforce cyber security practices every two quarters but did reinforce cyber security practices every three quarters. (2.6) OR	document or implement any processes for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.4. (2.4) OR The Responsible Entity did not implement any Cyber Security Incident response plans for assets with a low impact rating that included the topics as required by Requirement R2, Part 2.5. (2.5) OR The Responsible Entity did not implement a security awareness program

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				practices every three quarters. (2.6) OR The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 in more than 16 calendar months but less than or equal to 17 calendar months. (2.6)	The Responsible Entity did not reinforce the topics each 15 calendar months but reinforced the topics as required by Requirement R2, Part 2.6 for assets with a low impact rating in more than 17 calendar months but less than or equal to 18 calendar months. (2.6)	for assets with a low impact rating that collectively included the topics as required by Requirement R2, Part 2.6. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced cyber security practices at least every 15 months. (2.6) OR The Responsible Entity did not implement a security awareness program for assets with a low impact rating that reinforced the topics

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						within 18 calendar months as required by Requirement R2, Part 2.6. (2.6)
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but	The Responsible Entity has used delegated authority for actions where allowed by the CIP

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-6, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-6, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-6, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of the requirement is to outline a set of protections designed for all low impact BES Cyber Systems. The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed. The intent is that such protections are part of a program that covers the low impact BES Cyber Systems collectively either at a programmatic or site level, not an individual device or system level.

There are four main areas that must be covered by this security program: physical security, electronic access controls for all external routable protocol paths or Dial-up Connectivity, a security awareness program, and cyber security incident response plans.

The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary.

2.1 - As with Requirement R1, the number of policies and the specific language used in them would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas in CIP-003-6, Requirement R2, Parts 2.2 through 2.6. The Responsible Entity has flexibility in the number and structure of its policies to meet its needs and organization. Examples include developing a single comprehensive cyber security policy covering these topics for all in-scope assets, several comprehensive cyber security policies based on asset type, or a single high-level umbrella policy with additional policy detail in lower level documents in its documentation hierarchy.

2.2 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity’s controls.

2.4 – The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. The electronic access controls should address the risk of using the asset’s external connectivity to gain access to the low impact BES Cyber Systems. The entity should be able to describe how its electronic access controls on the external connectivity paths protect the collection of low impact BES Cyber Systems at the site. The intent is to reduce the risk of aggregation of numerous low impact BES Cyber Systems at the site or across multiple sites through external connectivity.

Examples of sufficient access controls may include:

- All the external routable protocol connectivity paths to the asset pass through a firewall that denies all traffic by default with explicit inbound and outbound access permissions defined, or equivalent method by which both inbound and outbound connections are shielded from or to the world-wide-web (e.g. IP addresses, ports, services, and data diode) for scenarios representative of the Responsible Entity's sites having Low Impact BES Cyber Systems.

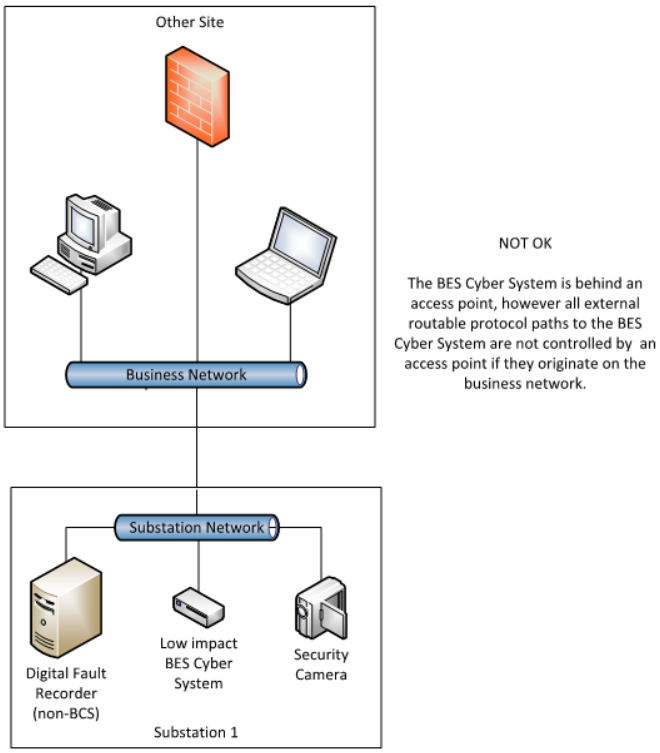
- Dialup Connectivity to a low impact BES Cyber System is set to dial out only (no autoanswer) to a preprogrammed number to deliver data. Incoming Dialup Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

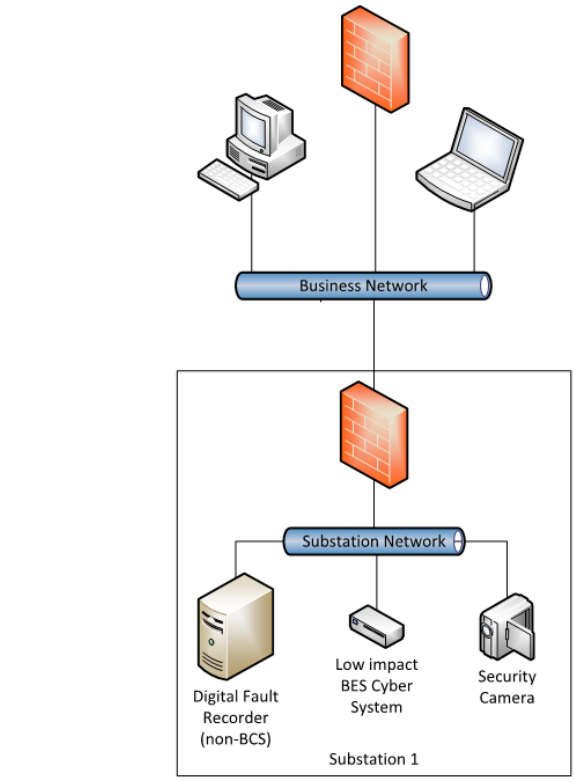
Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has dialup connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset which has a default password. There is no access control in this instance.
- An asset has external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.

The SDT also notes that in topic 2.4, the SDT uses the term “electronic access control” in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

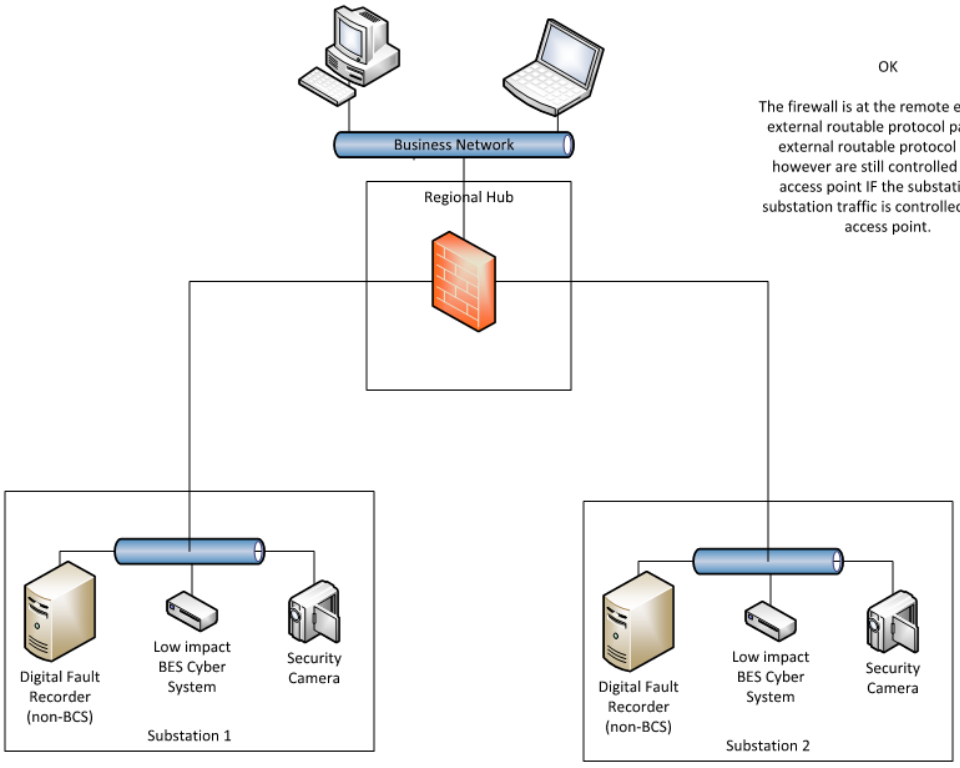
The following diagrams explain the SDT’s rationale.





OK

All the external traffic to the BES Cyber System is controlled by an access point.



OK

The firewall is at the remote end of an external routable protocol path. All external routable protocol paths however are still controlled by the access point IF the substation to substation traffic is controlled via the access point.

2.5 - The entity should have a documented cyber security incident response plan that includes each of the topics listed. For assets that have limited or no connectivity, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a cyber security incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as well as other forms of tabletop exercises or paper drills. NERC-led exercises such as GridEx participation would also count as an exercise if the entity's response plan is followed.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

2.6 - The intent of the security awareness program is for entities to reinforce good cyber security practices with their personnel on at least a quarterly basis. The physical security, electronic access controls, and the cyber security incident response plan should be covered at least every 15 months. It is up to the entity as to the topics and how it schedules these topics. It should be sufficient for an entity to produce the awareness material that it delivered quarterly and the delivery method(s) (posters, emails, topics at staff meetings, etc.). The intent is that tracking of reception of the messages by personnel is not required.

Requirement R3:

The intent of CIP-003-6, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-6, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to

the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.